CLAIMS

What is claimed is:

1. A method of excising a compromised node from a community of nodes capable of information sharing comprising:

broadcasting a new traffic encryption key to each of a plurality of top tier groups in a top level tier, wherein the plurality of top tier groups excludes a group that includes the compromised node; and

within the group that includes the compromised node, recursively broadcasting the new traffic encryption key to groups of nodes at a succession of lower tiers, until the compromised node is excised.

2. The method of claim 1 wherein broadcasting a new traffic encryption key to each of a plurality of top tier groups comprises:

for each group in the plurality of top tier groups, encrypting the new traffic encryption key using a tier-group specific key encryption key.

3. The method of claim 1 wherein each tier in a progression of lower tiers comprises a plurality of groups, one group of the plurality of groups including the compromised node, and wherein recursively broadcasting comprises:

for each tier in the succession of lower tiers, broadcasting the new traffic encryption key to a subset of the plurality of groups, such that the compromised node does not receive the new traffic encryption key.

4. The method of claim 1 wherein recursively broadcasting comprises:

broadcasting the new traffic encryption key to a plurality of lower tier groups in a lower tier, the plurality of lower tier groups excluding a lower tier group that includes the compromised node; and

within the lower tier group that includes the compromised node, broadcasting the new traffic encryption key to a plurality of nodes in a lowest tier, wherein the plurality of nodes excludes the compromised node.

5. The method of claim 4 wherein broadcasting the new traffic encryption key to the plurality of lower tier groups in the lower tier comprises:

for each of the plurality of lower tier groups, encrypting the new traffic encryption key using a tier-group specific key encryption key.

6. The method of claim 5 wherein the compromised node is a node coupled to a wireless communications system.

7. The method of claim 5 wherein the compromised node is a node coupled to the Internet.

8. A method of operating a key management center to excise a compromised node comprising:

from a list of top tier key encryption keys, selecting a top tier key encryption key that does not correspond to a group that includes the compromised node;

encrypting a new traffic encryption key using the top tier key encryption key, to produce an encrypted traffic encryption key; and

broadcasting a message that includes the encrypted traffic encryption key.

9. The method of claim 8 further comprising repeating the actions in the method for all top tier groups except the group that includes the compromised node.

10. The method of claim 8 further comprising:

within the group that includes the compromised node, broadcasting the new traffic encryption key to a plurality of nodes excluding the compromised node.

11. The method of claim 10 further comprising:

within the group that includes the compromised node, broadcasting new tier group key encryption keys to the plurality of nodes excluding the compromised node.

12. A key management center comprising:

an encryption device; and

a storage device coupled to the encryption device, the storage device being configured to hold a hierarchy of key encryption keys.

13. The key management center of claim 12 wherein the hierarchy of key encryption keys comprises:

a lowest level tier in which each of a first plurality of key encryption keys is assigned to a corresponding node.

14. The key management center of claim 13 wherein the hierarchy of key encryption keys further comprises:

a next higher level tier in which each of a second plurality of key encryption keys is assigned to a corresponding group of nodes.

15. The key management center of claim 13 wherein the hierarchy of key encryption keys further comprises:

a plurality of next higher level tiers wherein each of the plurality of next higher level tiers includes a separate plurality of key encryption keys, each of the separate plurality of key encryption keys being associated with a different plurality of key encryption keys on a next lower tier.